UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/010,743	12/06/2001	David W. Aucsmith	10559/463001/P10875	2946

20985 7590 12/28/2005

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
DERWICH, KRISTIN M	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/010,743	Applicant(s) AUCSMITH ET AL.	
	Examiner Kristin Derwich	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 September 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22,28-35 and 39-46* is/are pending in the application.

4a) Of the above claim(s) *23-27 and 36-38* is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22,28-35 and 39-46* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 December 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 23-27 and 36-38 are cancelled. Claims 1-22, 28-35 and 39-46 are pending.

Response to Amendment

Applicant's amendments with respect to previously presented claims 2-8, 10-16, 18, 20-22 and 31-35, amended claims 1, 9, 17, 19 and 28-30 and newly present claims 39-46 filed September 19, 2005 have been fully considered (MPEP 714.04; 37 CFR 1.111) but they are not persuasive. The Examiner would like to point out that this action is made final (See MPEP 706.07a).

Claim Objections

2. Amendments to the claims in order to correct the minor informalities are accepted. Therefore, the previous claim objections are withdrawn.

3. Claim 6 objected to because of the following informalities: Claim 6 is mistakenly marked as currently amended when it appears no changes have been made. Appropriate correction is required.

Response to Arguments

4. Applicant's arguments with respect to claims 1-46 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claim 40 rejected under 35 U.S.C. 102(e) as being anticipated by Lyle, U.S. Patent No. 6,886,102.

As per claim 40:

Lyle discloses a method comprising:

At a server, receiving from at least two remote clients indications of possible security problems at the clients (6:52-7:18); and

Determining in real time at the server an existence of an anomaly based on the indications of the possible security problems from the at least two remote client locations (6:52-7:18).

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-3, 6-8, 9-11 and 14-22 and 28-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack et al. (Shostack), U.S. Patent No. 6,298,445 in view of Lyle, U.S. Patent No. 6,886,102.

As per claim 1:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

determining at the home location an anomaly based on at least the possible security problem (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly based on information sent to the home location from at least one other client location and transmitting notice of the anomaly to the client location at which the possible security problem is detected. However, Lyle discloses a method wherein an event, which consists of an actual or suspected attack, is determined based on information gleaned from an internal source called a sniffer (6:52-7:18). Lyle also discloses a method wherein the responsive action, such as a message is sent to the device with the actual or suspected attack (8:21-59).

As per claim 9, this is a computer readable medium version of the claimed method discussed above in claim 1 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 2:

Shostack further discloses a method further comprising transmitting notice of the anomaly in real time to other client locations that may communicate with the home location over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 10, this is a computer readable medium version of the claimed method discussed above in claim 2 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 3:

Shostack further discloses a method further comprising notifying a firewall located between the client location and the home location about the anomaly (4:19-24, wherein the anomaly is an unauthorized user attempting to gain access to the network).

As per claim 11, this is a computer readable medium version of the claimed method discussed above in claim 3 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 6:

Shostack further discloses a method in which the anomaly includes unauthorized access to the network (4:64-67; 5:1, wherein this is an example of a security vulnerability (4:47-48) and the security vulnerabilities function as anomalies).

As per claim 14, this is a computer readable medium version of the claimed method discussed above in claim 6 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 7:

Shostack further discloses a method in which the anomaly includes unauthorized access of a resource accessible through the network (5:1-4, wherein the program library is a network resource).

As per claim 15, this is a computer readable medium version of the claimed method discussed above in claim 7 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 8:

Shostack further discloses a method in which the anomaly includes unauthorized use of resources available through the network (6:10-13, wherein seeing the disk is using a network resource).

As per claim 16, this is a computer readable medium version of the claimed method discussed above in claim 8 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 17:

Shostack discloses a method comprising:

At a home location in a network, receiving from a remote client location an indication of a possible security problem at the client (6:66-67; 7:1, the first application is used to transmit notice of possible security problems and the second application functions to receive information from the first application.) and determining in real time at the home location an existence of an anomaly based on at least the indication of the possible security problem (7:20-27, wherein the security vulnerabilities function as anomalies).

Shostack fails to teach determining at the home location an anomaly based on information sent to the home location from at least one other client location and transmitting notice of the anomaly to the client location at which the possible security problem is detected. However, Lyle discloses a method wherein an event, which consists of an actual or suspected attack, is determined based on information gleaned from an internal source called a sniffer (6:52-7:18).

As per claim 18:

Shostack further discloses a method further comprising transmitting notice of the existence of the anomaly in real time from the home location to the remote client location (7:57-63, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

As per claim 19:

Shostack further discloses a method further comprising notice of the existence of the anomaly in real time from the home location to other remote client locations that may communicate with the home location over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 20:

The method of claim further comprising notifying, from the home location, a firewall located between the remote client location and the home location about the anomaly.

As per claim 21:

Shostack further discloses a method of claim further comprising transmitting information from the home location to the remote client location to help the remote client location identify possible security problems (13:7-9, wherein the database updates to the security vulnerabilities helps to identify possible security problems).

As per claim 22:

Shostack further discloses a method further comprising determining the existence of the anomaly based on at least information regarding previous anomalies (9:56-63, wherein the database contains a log of all of the previous security vulnerabilities which function as anomalies).

As per claim 29:

Lyle further discloses an apparatus in which the first mechanism also determines the anomaly based on at least information regarding previously determined anomalies (7:66-8:11).

As per claim 30:

Shostack discloses a system comprising:

a client terminal (9:10);

a server (9:10);

a first client mechanism accessible by the client terminal to detect a possible security problem at the client terminal (6:43-46, wherein an intrusion is a possible security problem);

a second client mechanism accessible by the client terminal to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem);

a third client mechanism accessible by the client terminal to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems (7:57-63; 9:10-21, wherein the client receives the software enhancement updates which function as updates from the server about security problems);

a first server mechanism accessible by the server to determine an anomaly based on at least information from a client regarding a possible security problem (7:15-16, wherein the security vulnerabilities function as anomalies and the local server is the home location); and

a second server mechanism accessible by the server to transmit notice of the anomaly in real time over the network to the client terminal (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly based on information sent to the home location from at least one other client location and transmitting notice of the anomaly to the client location at which the possible security problem is detected. However, Lyle discloses a method wherein an event, which consists of an actual or suspected attack, is determined based on information gleaned from an internal source called a sniffer (6:52-7:18). Lyle also discloses a method wherein the a responsive action, such as a message is sent to the device with the actual or suspected attack (8:21-59).

As per claim 28 this is an apparatus version of the claimed system discussed above in claim 30 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 32:

Shostack further discloses a system in which the first server mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies (9:56-63, wherein the database contains a log of all of the previous security vulnerabilities which function as anomalies).

As per claim 33:

Shostack further discloses a system in which the second server mechanism is also configured to transmit notice of the anomaly in real time to other client locations that may communicate with the server over the network (6:58-59, wherein information about the network status includes anomalies found).

As per claim 34:

Shostack further discloses a system further comprising a firewall located between the client terminal and the server and configured to act as an intermediary for information flowing between the client terminal and the server (4:19-24, since the server is remotely connected to the network 20 (9:13-14; fig 2, item 20), the placement of the firewall makes it an intermediary between the external server and the client, therefore, the firewall's functionality as a filter shows that information flows between the server and client).

As per claim 39:

Lyle further discloses a method wherein information is sent to a home location from the other client location comprising a notice of a possible security problem at the other client location (6:52-6:18).

As per claim 41:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly based on the possible security problem by searching for particular information in the anomaly. However, Lyle discloses searching for a particular file type associated with a known intrusion technique (10:44-59).

As per claim 42:

Shostack discloses a method comprising:

detecting a possible security problem at a client location (6:43-46, wherein an intrusion is a possible security problem);

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the location (6:53-57, wherein sending an alarm functions as transmitting notice of the possible security problem and the system administrator resides at a home location which is the local server);

transmitting notice of the anomaly in real time to the client location (7:57-63; 9:10-21, wherein the software enhancement being sent is the notice of the security vulnerability, which functions as the anomaly).

Shostack fails to teach determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location. However, Lyle discloses a method wherein the event, which consists of an attack, is compared to other events that have occurred (7:50-8:11).

As per claims 45 and 46:

Lyle further discloses a method wherein a wide view mechanism such as an analysis framework module, collects and maintains information regarding events reported to the server (7:50-65) which includes a statistics mechanism to compute and store records of events (8:12-20).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), not only do vulnerabilities updates need to be disseminated, but tracking the hacker who breached the security is also essential in the security of a system against intrusions in order t ensure that the same person cannot do so again.

7. Claims 4, 12, 24, 27 and 31 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) as applied to claims 1, 9, 23, 26 and 30 above and further in view of Baker, U.S. Patent No. 6,775,657.

As per claim 4:

Shostack and Lyle fail to teach a method further comprising inspecting a packet that arrives at the client location to detect the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 12, this is a computer readable medium version of the claimed method discussed above in claim 4 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 24:

Shostack and Lyle fail to teach a method further comprising inspecting a packet that arrives at the client location to detect the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 27:

Shostack and Lyle fail to teach an apparatus in which the first mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

As per claim 31:

Shostack and Lyle fail to teach a system in which the first mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem. However, Baker discloses a method wherein a network based intrusion detection system analyzes network packet data to make security decisions (1:41-42; 46-53). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to analyze a packet that arrives at the client in order to make security decisions because this would make the intrusion detection system scale well for network protection since it is the amount of traffic that determines performance, therefore it would also be easier to control and improve performance of the network as a whole (1:53-60).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), not only do vulnerabilities updates need to be disseminated, but tracking the hacker who breached the security is also essential in the security of a system against intrusions in order t ensure that the same person cannot do so again.

8. Claims 5, 13 and 35 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) as applied to claims 1, 9 and 30 above and further in view of Bowman-Amuah, U.S. Patent No. 6,697,824.

As per claim 5:

Shostack and Lyle fail to teach a method in which the network includes a virtual private network. However, Bowman-Amuah discloses a method wherein a network is protected from unauthorized access through the encryption services provided by Virtual Private Networking (75:64-65, fig 36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a virtual private network with the network because of the added security benefits a VPN affords a system against unauthorized users.

As per claim 13, this is a computer readable medium version of the claimed method discussed above in claim 5 wherein all claimed limitations have also been addressed and/or cited as set forth above.

As per claim 35:

Shostack and Lyle fail to teach a system in which the firewall includes a corporate server. However, Bowman-Amuah discloses a method wherein a corporate firewall includes a corporate server at a corporate headquarters (75:65-66; 76:19-23). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include a corporate server with the firewall because if the intrusion detection system were to be used in a business setting the firewalls would provide increased access control for the internal network (76:21-23).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle because in order to make a system less vulnerable to attack as stated in Shostack (2:18-28), not only do vulnerabilities updates need to be disseminated, but tracking the hacker who breached the security is also essential in the security of a system against intrusions in order t ensure that the same person cannot do so again.

9. Claims 43 and 44 rejected under 35 U.S.C. 103(a) as being unpatentable over Shostack (U.S. 6,298,445) in view of Lyle (U.S. 6,886,102) as applied to claims 42 above and further in view of Moran, U.S. Patent No. 6,826,697.

As per claims 43 and 44:

Shostack and Lyle fail to teach a method in which determining the anomaly comprises searching for non-standard access patterns such as a login from an unexpected user. However, Moran discloses a method wherein failed login attempts are logged (19:41-20:18). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to combine the inventions of Shostack and Lyle with Moran because in order to make a system less vulnerable to attack as stated in Shostack (2:18-

28), the ability to detect further types of attacks such as forward and backward time steps in a log file or an overflow buffer attack as stated in Moran (4:1-37) would increase the security against attacks as a whole.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin Derwich whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kristin Derwich
Examiner
Art Unit 2132

KMD
KMD

Gilberto B

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100